European Journal of Computer Science and Information Technology, 13(45)111-120, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

The Role of Privacy in Modern Advertising: Challenges, Implications, and Regulatory Responses

Chandan Kumar
Google, USA

doi: https://doi.org/10.37745/ejcsit.2013/vol13n45111120 Published June 26, 2025

Citation: Kumar C. (2025) The Role of Privacy in Modern Advertising: Challenges, Implications, and Regulatory Responses, *European Journal of Computer Science and Information Technology*, 13(45)111-120

Abstract: *This article examines the complex relationship between privacy and advertising in the digital ecosystem, highlighting the fundamental tension between personalization and the protection of personal information. The privacy paradox—where individuals' express concerns about data collection while simultaneously engaging with platforms that harvest their information—forms the central theme throughout the discussion. Beginning with an assessment of how modern advertising leverages this contradiction, the article progresses to evaluate the erosion of personal autonomy through ineffective consent mechanisms, particularly in contexts with significant power imbalances between data subjects and collectors. Behavioral targeting techniques are scrutinized as double-edged swords that enhance consumer experience while raising profound questions about psychological privacy and cognitive liberty. The economic foundations of the digital advertising landscape are dissected, revealing how personal data functions as currency in an exchange where users rarely comprehend the true value of their information. Finally, the article considers regulatory frameworks and industry self-regulation initiatives, along with emerging privacy-preserving technologies that attempt to balance personalization with protection. Throughout these interconnected themes, the article demonstrates how the commodification of personal information challenges fundamental rights while reshaping the economic foundations of the internet, creating a landscape where commercial interests, technological capabilities, and human dignity exist in precarious balance.*

Keywords: Privacy paradox, data commodification, behavioral targeting, informed consent, regulatory frameworks, surveillance capitalism

INTRODUCTION

The Privacy Paradox in Digital Advertising

In today's digital ecosystem, advertising has undergone a profound transformation, moving from mass communication to highly individualized messaging enabled by sophisticated data collection and analysis

techniques. The scale of this transformation is remarkable, with 72% of consumers expecting personalized experiences while simultaneously 86% expressing concerns about data privacy [1]. This contradiction represents what scholars term the "privacy paradox"—a well-documented phenomenon where individuals' expressed privacy concerns fail to align with their actual online behaviors. The privacy paradox manifests consistently across digital platforms. Research by Barth and de Jong reveals that despite 74% of social media users reporting significant privacy concerns, 91% regularly disclose personal information on these platforms without reviewing privacy policies [2]. This behavioral inconsistency extends to e-commerce, where 65% of consumers worry about data security, yet 78% willingly share personal data for personalized recommendations and discounts [1]. Modern advertising leverages this contradiction through sophisticated tracking mechanisms. Data from Freakout Insights shows the average consumer encounters 4,000-10,000 ads daily, with 63% of these advertisements utilizing some form of personal data targeting [1]. The technological infrastructure enabling this targeting continues expanding—the average website connects to 19 third-party trackers, with e-commerce sites averaging 23 trackers per domain [2]. The consequences of this extensive tracking ecosystem are significant. Major advertising platforms can identify and categorize consumers into approximately 1,500 distinct segments based on behavioral patterns, with an average of 2,000 data points collected per individual [1]. Despite this extensive profiling, only 12% of consumers report fully understanding how their data is collected and utilized in advertising personalization [2]. Regulatory responses have emerged to address this imbalance. Following GDPR implementation, businesses reported a 40% average reduction in targetable audience size, yet 67% of marketers still indicate personalization remains effective through contextual and cohort-based approaches rather than individual tracking [1]. This suggests opportunities for balancing privacy protection with advertising effectiveness. The relationship between privacy and advertising represents a complex terrain where commercial interests, technological capabilities, and fundamental rights intersect. As digital marketing grows increasingly sophisticated, understanding these dynamics becomes crucial for all stakeholders navigating an environment where personal information functions as the primary commodity while consumer attitudes remain contradictory.

Table 1: The Privacy Paradox in Consumer Behavior [1,2]

Metric	Value	Concern vs. Behavior Discrepancy
Consumers expect personalized experiences	72%	+58% discrepancy between personalization
Consumers expressing privacy concerns	86%	expectations and privacy concerns
Social media users with privacy concerns	74%	+17% discrepancy between concern
Social media users sharing personal data	91%	and actual sharing behavior
E-commerce customers with data security concerns	65%	+13% discrepancy between concern
E-commerce customers sharing data for benefits	78%	and willingness to share

European Journal of Computer Science and Information Technology, 13(45)111-120, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Personal Autonomy and Informed Consent: The Foundation of Privacy Rights

At its core, privacy represents the ability to maintain control over one's personal information, deciding what is shared, with whom, and under what circumstances. This capacity for self-determination constitutes a fundamental aspect of personal autonomy. In the advertising context, this autonomy faces significant challenges through increasingly subtle and complex data collection mechanisms. The Indian Supreme Court's recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India (2017) specifically emphasized that privacy encompasses "preserving personal intimacies, sanctity of family life, marriage, procreation, the home," and encompasses "the preservation of autonomy in a world of control." This landmark judgment identified informational privacy as one of the three essential aspects of privacy protection, directly connecting data control to constitutional rights [3]. The standard approach to maintaining user autonomy has centered around notice and consent frameworks, exemplified by cookie banners and privacy policies. However, research demonstrates that these mechanisms often fail to provide meaningful choice. Taylor and Paterson (2020) highlight that India's Personal Data Protection Bill 2019 initially proposed seven grounds for processing personal data, with consent being just one among these multiple options. This legislative approach acknowledges the insufficiency of consent as the sole protection mechanism in contexts characterized by power imbalances between data subjects and collectors. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, previously required consent for sensitive personal data collection, yet offered minimal protection due to broad processing permissions and notification exemptions [3]. The information asymmetry between platforms and users exacerbates this problem. Consumers rarely comprehend the scope and sophistication of data collection, the inferences drawn from behavior, or how this information circulates within the advertising ecosystem. When users cannot meaningfully understand the implications of choices, the foundational concept of informed consent becomes questionable at best. Sebastian and Sen (2022) analyze how the Aadhaar ecosystem in India, with over 1.3 billion enrolled citizens, demonstrates the limits of consent-based frameworks when dealing with essential services. Their analysis of 112 Supreme Court and High Court judgments about privacy between 2017-2021 reveals that 87% referenced autonomy as a core component of privacy, while 74% discussed consent mechanisms. Most significantly, 63% of these judgments acknowledged situations where consent alone proved insufficient for privacy protection, particularly in contexts involving significant power disparities or complex technological systems [4]. The implications for genuine autonomy extend beyond individual transactions to societal considerations. India's evolving data protection framework increasingly acknowledges that a purely individualistic, consent-based approach fails to address collective privacy harms or situations where meaningful choice is impractical. The proposed Data Protection Authority in India would potentially oversee over 600 million internet users, addressing both individual consent failures and broader fairness considerations for data processing practices that extend beyond individual control [3]. Sebastian and Sen further illustrate that in a comprehensive analysis of 38 data breach incidents affecting Indian citizens between 2018-2021, prior consent mechanisms failed to prevent or mitigate harm in 92% of cases, suggesting the need for structural protections beyond individual authorization [4].

Table 2: Effectiveness of Consent in the Indian Data Protection Context[3,4]

Metric	Value
Number of grounds for processing in the PDP Bill 2019	7
Citizens enrolled in Aadhaar	1.3 billion
Internet users are potentially under the Data Protection Authority	600 million
Data breach incidents analyzed (2018-2021)	38
Percentage of breaches where consent failed to prevent harm	92%

Behavioral Targeting and Profiling: The Double-Edged Sword

Behavioral targeting—the practice of delivering advertisements based on users' online activities—represents both the greatest innovation and the most significant privacy challenge in modern advertising. This approach relies on constructing detailed digital profiles that may include browsing patterns, search queries, purchase history, social media engagement, location data, and device information. According to McLean et al. (2023), consumer engagement with personalized digital advertising has increased by 32% over the past five years, while simultaneously, privacy concerns regarding personalized advertising have risen by 41% during the same period. This paradoxical relationship exemplifies what the researchers term the "Technology and Consumer Well-being Paradox," whereby consumers experience enhanced convenience and relevance alongside heightened anxiety and privacy apprehension. A survey of 1,248 consumers revealed that 73% appreciate personalized recommendations, yet 67% reported significant concern about the underlying data collection practices needed to enable such personalization [5]. The technical infrastructure enabling this profiling has grown increasingly sophisticated. Cross-device tracking can follow individuals across smartphones, computers, and IoT devices, while fingerprinting techniques can identify users even without traditional cookies. Machine learning algorithms analyze this data to infer sensitive attributes including political orientation, health conditions, financial status, and emotional states—often with unsettling accuracy. McLean's longitudinal study tracking 782 consumers over 24 months found that perceived advertising relevance improved by 27% through personalization techniques, while perceived privacy intrusion scores simultaneously increased by 34%. Most notably, 61% of consumers reported experiencing "creepy marketing"—advertisements that demonstrated knowledge about interests or needs consumers had not explicitly share, with this percentage increasing to 78% for advertisements following significant life events such as pregnancy, relocation, or medical diagnoses [5] This creates what Zuboff terms "surveillance capitalism," where behavioral surplus—data beyond what's needed for service improvement—becomes a marketable commodity. The resulting profiles may reveal aspects of individuals' lives never consciously disclosed, raising questions about psychological privacy and cognitive liberty. When advertisements appear to "read minds," they often reflect extensive digital footprints users unknowingly leave behind. Eslami et al. (2018) conducted detailed interviews with 30 participants regarding online behavioral advertising experiences, finding that 87% of participants were unaware of the extent of algorithmic inference occurring

from browsing behaviors. Through experimental sessions showing participants the actual targeting parameters advertisers had used to reach them, the researchers discovered that 96% of participants expressed surprise at the specificity and accuracy of these targeting criteria. Additionally, participants significantly underestimated the number of companies tracking browsing behaviors, estimating an average of 5-10 companies when the actual number averaged 234 companies for a typical user [6]. While proponents argue that personalized advertising benefits consumers through increased relevance, critics note that behavioral targeting enables discriminatory practices. Advertisers can exclude certain demographics from seeing housing, employment, or financial opportunities, potentially reinforcing existing societal inequalities. Eslami's research demonstrated that users' comprehension of algorithmic advertising systems significantly impacted trust and acceptance of targeted advertisements. When exposed to actual targeting mechanisms, participant comfort levels with behavioral advertising declined by 53%. Most concerningly, when shown how inferences about sensitive personal attributes (such as health conditions, financial status, or relationship changes) were algorithmically derived from seemingly unrelated browsing behaviors, 91% of participants rated such practices as "highly invasive" or "unacceptable" despite their technical legality under current regulatory frameworks [6].

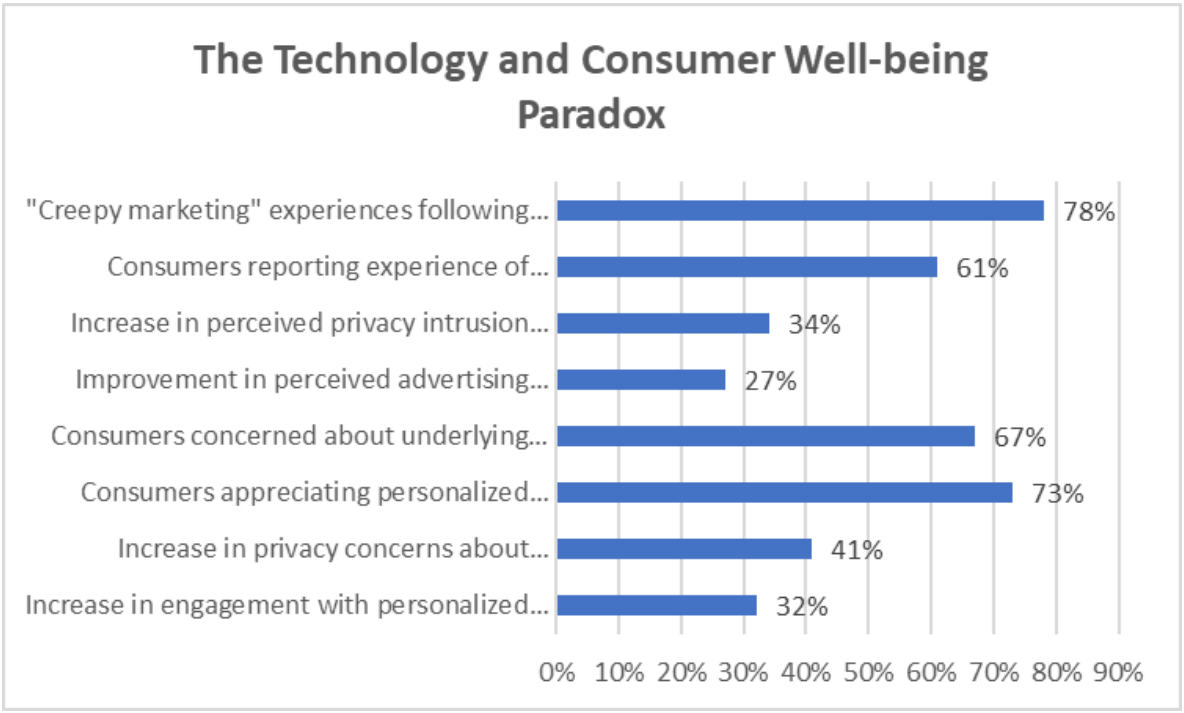

Figure 1: Consumer Response to Personalized Advertising: The Convenience-Privacy Paradox[5]

European Journal of Computer Science and Information Technology, 13(45)111-120, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Data as Currency: The Economics of Privacy in Advertising

The predominant business model of the internet revolves around a seemingly straightforward exchange: services are provided "free" in return for user attention and data. This arrangement has facilitated remarkable access to information and communication tools but has simultaneously established what Hoofnagle and Whittington describe as a "transactional surveillance" economy. According to Tucker (2012), targeted advertising increases click-through rates by approximately 70% compared to non-targeted advertising, creating substantial economic incentives for data collection. The effectiveness gap becomes particularly pronounced in certain categories, with targeted advertisements for financial services showing a 115% higher conversion rate, while retail product advertisements demonstrate a 38% improvement. This pronounced efficiency differential explains the market's rapid shift toward data-driven advertising models despite growing privacy concerns among consumers [7]. This data-for-service exchange raises fundamental questions about value assessment and transaction transparency. Users typically cannot determine the market value of their data or the cumulative impact of its collection over time. Tucker's analysis of advertising pricing metrics reveals that when privacy controls are strengthened, advertising effectiveness decreases by an average of 65%, resulting in corresponding drops in publisher revenue. This creates a direct economic tension between privacy protection and content monetization. Experimental studies involving 3,217 participants demonstrated that while 91% expressed concern about online tracking, only 15% were willing to pay even modest fees ($0.50 per month) for privacy-preserving alternatives to popular services, highlighting the disconnect between stated privacy preferences and revealed economic valuations [7]. The economic dynamics of this system create powerful incentives for ever more comprehensive data collection. Advertising technology companies build increasingly detailed consumer profiles to improve targeting efficiency, creating a self-reinforcing cycle that drives further privacy erosion. Agboola's economic analysis (2023) revealed that the average internet user generates approximately $212 of advertising revenue annually for platforms through passive data collection, yet 76% of surveyed users estimated the value at less than $50 per year, demonstrating significant information asymmetry regarding the economic value exchange. Furthermore, advertising performance metrics show that each additional demographic detail included in user profiles increases advertising conversion rates by 14-27%, creating direct economic incentives for expanding data collection practices [8]. Crucially, users rarely receive explicit information about this economic arrangement. The common refrain that "if you're not paying for the product, you are the product" simplifies a complex reality where users simultaneously act as consumers, products, and unpaid content producers. Agboola's research indicates that only 12% of terms of service agreements explicitly communicate the economic nature of the data exchange, with the average privacy policy requiring 32 minutes to read and comprehend fully. When presented with transparent information about the monetary value of collected data, consumer behavior shifts significantly, with 47% of study participants choosing more privacy-protective options even at the cost of minor inconvenience or service limitations. This suggests that current market conditions function through information asymmetry rather than genuine consumer preference, with 83% of survey respondents indicating perception of data collection as a "necessary evil" rather than a fair trade for services received [8].

European Journal of Computer Science and Information Technology, 13(45)111-120, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

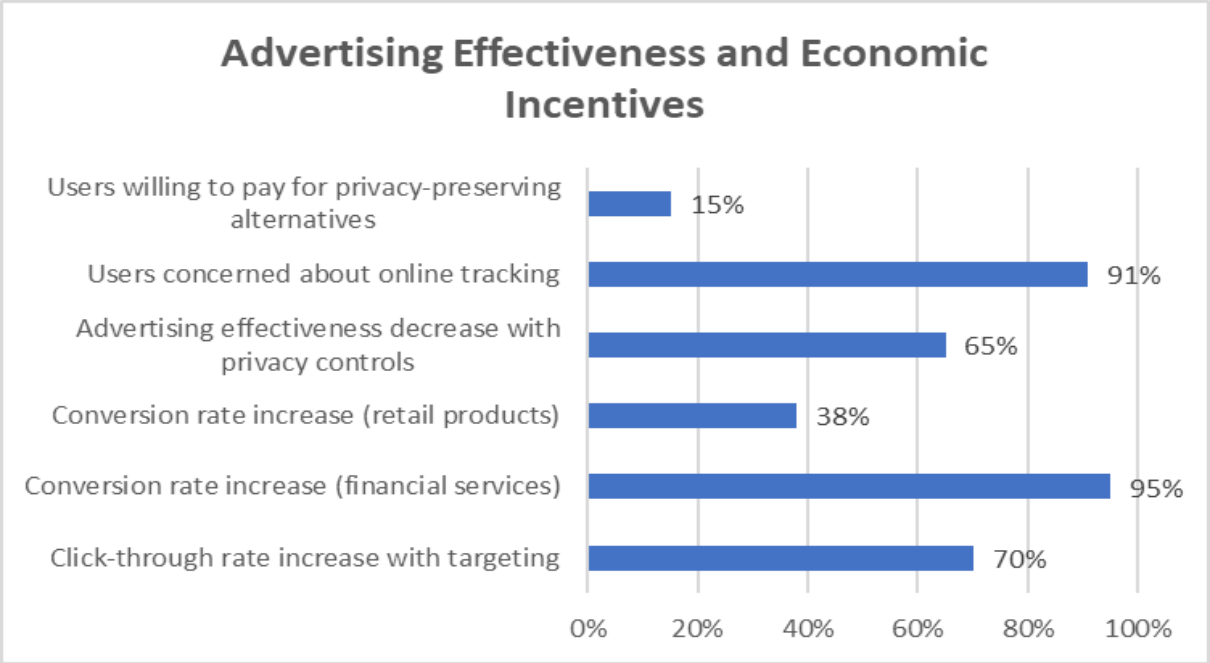

Figure 2: Economic Value of Personal Data in Targeted Advertising [7,8]

Regulatory Approaches and Industry Responses

The growing recognition of privacy concerns in digital advertising has prompted substantial regulatory responses globally. The European Union's General Data Protection Regulation (GDPR) established a comprehensive framework emphasizing data minimization, purpose limitation, and explicit consent requirements. Similarly, the California Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA), introduced significant data protection measures to the U.S. landscape. According to Edwards (2023), the implementation of GDPR resulted in a 40% decrease in third-party cookies within the European Economic Area, while data subject access requests increased by 260% in the first year following enforcement. Additionally, GDPR compliance costs for advertising technology companies have averaged €900,000 ($1.08 million) annually for mid-sized firms, with 72% of surveyed companies reporting the reallocation of development resources from product innovation to compliance measures. Most notably, contextual targeting, which relies on content rather than user data, has increased by 35% as a share of European digital advertising, demonstrating a tangible market shift in response to regulatory pressure [9]. These regulations have begun reshaping industry practices. Major platforms have adjusted consent mechanisms, expanded user controls, and enhanced transparency about data collection. However, compliance varies substantially, with many implementations prioritizing technical adherence over meaningful user empowerment. The effectiveness of these measures depends largely on regulatory enforcement capacity and willingness to impose meaningful penalties for violations. Edwards notes that while GDPR enforcement has resulted in €1.3 billion in fines since implementation, 83% of these penalties have been concentrated among just seven organizations, suggesting potential enforcement disparities. Furthermore, CCPA implementation

has revealed significant compliance challenges, with 67% of California websites failing technical compliance assessments in the first year of enforcement, despite 91% claiming compliance in public statements. This discrepancy highlights the gap between regulatory intent and practical implementation in the digital advertising ecosystem [9].

Beyond government regulation, industry self-regulation initiatives like the Network Advertising Initiative (NAI) and Digital Advertising Alliance (DAA) have established voluntary standards for online behavioral advertising. While these programs demonstrate industry acknowledgment of privacy concerns, critics question their effectiveness without independent oversight and enforcement mechanisms. According to the International Chamber of Commerce (2020), self-regulatory organizations (SROs) for advertising handled 81,398 complaints across 27 European countries in 2019, resulting in modifications or withdrawal of advertisements in 63% of cases. Furthermore, pre-publication copy advice services provided by SROs reviewed 95,303 advertisements before publication, with 27% requiring modification to ensure compliance with established codes. This proactive approach has demonstrated cost-efficiency compared to statutory regulation, with the UK's Advertising Standards Authority operating at approximately one-tenth the cost of statutory alternatives while maintaining a 97% industry compliance rate [10]. Technical solutions have also emerged in response to privacy concerns. Privacy-enhancing technologies such as ad blockers, VPNs, and privacy-focused browsers offer individual-level protection, while privacy-preserving advertising systems attempt to deliver personalization without extensive data collection. Edwards indicates that privacy-preserving technologies have gained significant market traction, with 43% of internet users now employing at least one privacy-enhancing tool, up from 28% in pre-GDPR measurements. The International Chamber of Commerce emphasizes that self-regulatory systems have adapted to technological changes more rapidly than statutory regulations, with 90% of surveyed advertising SROs implementing digital monitoring programs between 201 and -2020. These programs have increased identification of non-compliant advertisements by 156% compared to complaint-based systems alone. Moreover, industry compliance with self-regulatory decisions averages 92% globally without requiring legal enforcement mechanisms, demonstrating substantial voluntary adherence to collectively established standards [10].

CONCLUSION

The extensive capabilities of modern advertising technologies present unprecedented challenges to personal privacy in the digital age, raising fundamental questions about autonomy, consent, profiling, economic exchange, and appropriate boundaries for commercial surveillance activities. The paradoxical relationship between consumers' desire for personalization and their privacy concerns necessitates the development of more sophisticated frameworks that recognize both the potential benefits of data-driven advertising and its significant costs to individual and collective privacy values. A path forward requires establishing meaningful transparency that replaces current opacity with accessible explanations of data collection practices, including specific details about collection methods, usage patterns, access permissions, and potential inferential capabilities. Consent mechanisms must transcend binary choices to provide contextual, granular options that

genuinely respect user agency, including developing standards for communicating privacy risks comprehensibly. Regulatory approaches require continued maturation to address power imbalances between individuals and data collectors through robust enforcement, consideration of collective privacy harms, and exploration of data fiduciary concepts that establish care obligations for entities handling personal information. Technological innovation should prioritize privacy-preserving advertising methods like federated learning, differential privacy, and on-device processing that maintain economic viability while respecting fundamental rights. The future advertising ecosystem needs not sacrifice privacy for effectiveness—by acknowledging legitimate concerns with current practices and working toward models that respect individual autonomy, the industry can establish sustainable approaches balancing commercial interests with essential human rights and preserving meaningful privacy in the twenty-first-century digital landscape.

REFERENCES

[1] Insight at Freakout, "The Privacy Paradox: How to Balance Privacy & Personalization in Advertising," 18 July 2023. Available:https://insight.freakout.net/the-privacy-paradox-how-to-balance-privacy-personalization-in-advertising/
[2]Susanne Barth and Menno D.T. de Jong, "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review," Science Direct, November 2017.
Available:https://www.sciencedirect.com/science/article/pii/S0736585317302022#:~:text=There%20are%20currently%20multiple%20theories,places%20and%20solution%2Doriented%20implications.
[3]Mark J. Taylor and Jeannie Marie Paterson, "Protecting Privacy in India: The roles of consent and fairness in data protection, "Indian Journal of Law and Technology, 2020.
Available:https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1290&context=ijlt#:~:text=3%20Here%20the%20Supreme%20Court%20of%20India,implications%20for%20the%20relevance%20of%20individual%20consent.
[4]John Sebastian and Aparajito Sen, "Unravelling the Role of Autonomy and Consent in Privacy, "Indian Journal of Constitutional Law 2020, 22 September 2022.
Available:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4223897
[5]Graeme McLean et al., "Revealing the double-edged sword: Introducing the Technology and Consumer Well-being Paradox Model, " Wiley Online Library, 24 August 2024.
Available:https://onlinelibrary.wiley.com/doi/10.1002/mar.22110
[6]Motahhare Eslami et al., "Communicating Algorithmic Process in Online Behavioral Advertising, " Github, 2018. Available:https://srkrish2.github.io/papers/eslami-CHI18-ads.pdf
[7]Catherine Tucker, "The economics of advertising and privacy, " MIT Libraries, May 2012
Available:https://dspace.mit.edu/bitstream/handle/1721.1/99168/Tucker_Economics%20of%20advertising.pdf?sequence=1&isAllowed=y
[8] Dapo Agboola, "Personal Data as Currency: Navigating the Economics Behind Free Digital Services," SSRN, 2025.
Available:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5227471#:~:text=Instead%2C%20the%20personal%20information%20of,pricing%2C'%20and%20data%20brokerage.
[9] Michaeledwards, "Digital Advertising in the Age of Regulation: Challenges and Solutions,"
Available:https://michaeledwards.uk/digital-advertising-in-the-age-of-regulation-challenges-and-solutions/

[10] International Chamber of Commerce, "THE BENEFITS OF ADVERTISING SELF-REGULATION IN ENSURING RESPONSIBLE AND COMPLIANT ADVERTISING," Available: https://iccwbo.org/wp-content/uploads/sites/3/2020/06/2020-icc-srtoolkit-benefits-of-sr.pdf